

CORONAVIRUS: A Breeding Ground for Scams



- ▶ Prepared by John Andrew Singer, retired Senior Attorney, United States Federal Trade Commission, Bureau of Consumer Protection, March 30, 2020

Coronavirus-Generated Scams

- ▶ Crises often bring out the best in people
- ▶ They also provide opportunities for the “bottom feeders” of society to take advantage of others’ vulnerabilities and try to steal your money
 - ▶ Can be obvious, like price gouging



- ▶ Or may be more dangerous “subtle scams”

How “Bottom Feeders” Take Your Information

- ▶ Scammers get you to provide financial information and personally identifiable information.
- ▶ **Financial Information** includes: credit cards, debit cards, banks accounts, brokerage accounts, etc.
- ▶ **Personally Identifiable Information (PII)** is information that, either alone or when combined with publicly available information, can be used to identify a specific individual. PII includes: your name, social security number, driver’s license number, date of birth, address, personal email, personal phone number, financial account information.

How “Bottom Feeders” Hack Your Devices



How “Bottom Feeders” Hack Your Devices

- ▶ Scammers convince you unknowingly to install malware on your computer or other electronic devices
- ▶ You may install the malware by clicking on links, opening attachments or installing applications
- ▶ Once loaded onto your computer or other electronic device, malware can then transmit information about you to the scammer
- ▶ Malware also may “lock” your computer or other electronic device and the scammer will release it only if you pay ransom

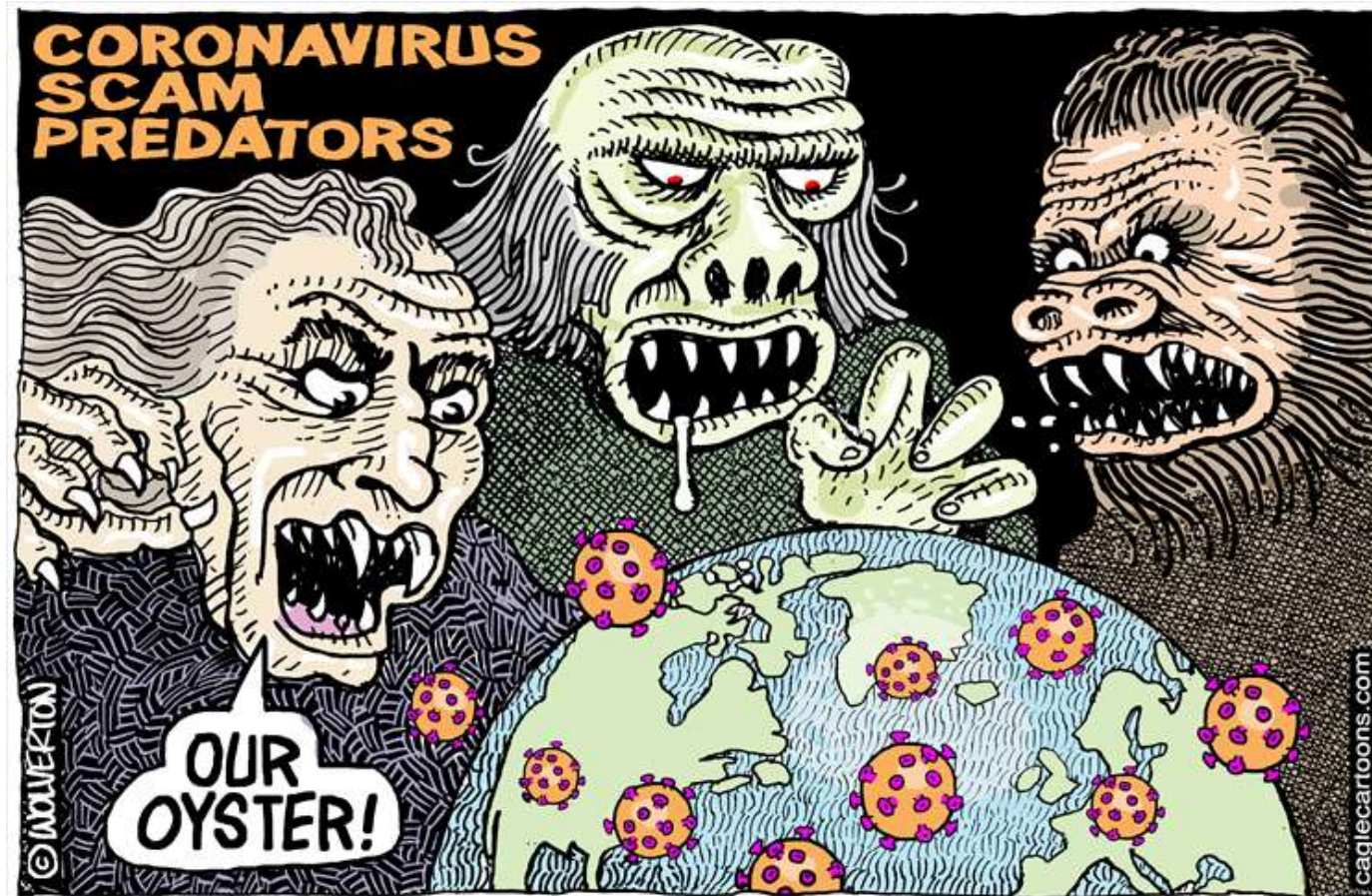
How “Bottom Feeders” Steal Your Money

- ▶ One-time payments for useless or non-existent goods or services that are worthless or that you never receive
- ▶ By tapping into and draining your credit cards and financial accounts

Note: Federal law limits your liability on credit card fraud to \$500. This limitation does **not** apply to debit cards.

- ▶ Using your PII to steal your identity and open new accounts and lines of credit in your name without your knowing

Coronavirus-Generated Scams



Coronavirus-Generated Scams

- ▶ Immoral opportunists pose as “helpers” and deceptively and egregiously prey on consumers in times of crises
- ▶ Anyone can fall victim to these scans, they are are very well-designed and can sometimes fool even sophisticated members of public
- ▶ Studies show that seniors are especially susceptible to scams as they tend to be more trusting
- ▶ While many of these scams are through unsolicited emails and texts, there has been a 49% increase in unsolicited telephone calls (primarily robocall) scams since the beginning of February when fear of coronavirus became more widespread

Top Four Coronavirus Scam Complaints

From the Better Business Bureau, as of March 20, 2020:

1. Sales of face masks
2. Fake cures
3. Government issued stimulus funds
4. Price gouging

Coronavirus Information Scams

- ▶ You will get an email or text from what appears to be a legitimate government organization
 - ▶ National Institutes for Health
 - ▶ Centers for Disease Control and Prevention
 - ▶ World Health Organization
 - ▶ Johns Hopkins (especially relating to the School of Public Health's coronavirus tracking map)
- ▶ Many of these emails are carefully crafted to look as if they are from a legitimate organization
 - ▶ Email typically will purport to provide “urgent,” “critical,” or similar information and updates
 - ▶ All you need to do to get this information is to click on a link or open an attachment

Coronavirus Information Scams, cont.

- ▶ Sometimes these emails refer to what appears to be seemingly real but actually non-existent laws. For example:
 - ▶ National Covid-19 Relief Act
 - ▶ Beat Coronavirus Act of 2020
 - ▶ Families First Coronavirus Relief Act
- ▶ **Clicking on the link or opening the attachment in the email or text will result in the scammer loading malware on to your computer or other electronic device**
- ▶ **Be equally wary of any apps that you can download that purport to provide this type of information**

Avoiding Coronavirus Information Scams

- ▶ Never respond to or click on links contained in unsolicited emails from unknown senders
- ▶ Carefully look at the sender's address or URL. Notice anything that looks out of place, for example:
 - ▶ *CDC-gov.org*
 - ▶ *WHO.com*
 - ▶ No information about sender
- ▶ Be aware that these types of scams often contain typos, poor grammar, LOTS OF CAPITAL LETTERS, and other non-standard English

Coronavirus Information Scam Example

**Distributed via the CDC Health Alert Network*

January 31, 2020

CDCHAN-00426

Dear [REDACTED]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (<https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html>)

You are immediately advised to go through the cases above for safety hazard

Sincerely,

CDC-INFO National Contact Center


National Center for Health Marketing

Division of eHealth Marketing

*Centers for Disease control and Prevention**

Coronavirus Information Scam Example

Singapore Specialist : Corona Virus Safety Measures

 **DT**
Tuesday, 28 January 2020 at 03:51
[Show Details](#)

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

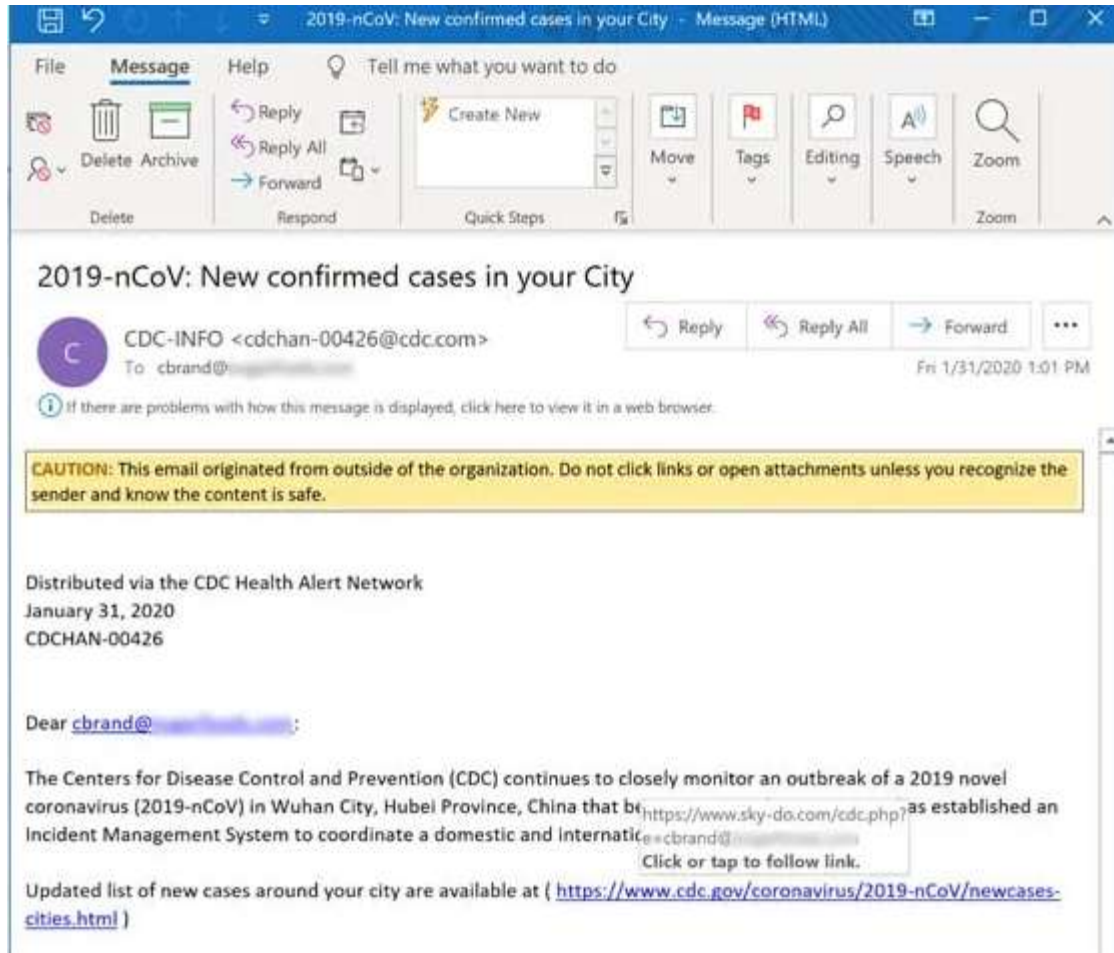
Use the link below to download

[Safety Measures.pdf](#)

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [Redacted]
Specialist wuhan-virus-advisory
[Redacted]
[Redacted]
[Redacted]
[Redacted]

Coronavirus Information Scam Example



Coronavirus Test Scams

- ▶ BACKGROUND INFO: There is a shortage of coronavirus tests in the United States. Coronavirus tests are available only through legitimate health care providers. There currently are no “at home” tests available for coronavirus.
- ▶ Do not fall victim to anyone offering to sell or provide you with a coronavirus test
 - ▶ May occur via email, text, robocall or even in person
 - ▶ Getting tested may seem risk-free because the test kit is “free” as a public service with you only having to pay nominal shipping and handling fee
 - ▶ Example of robocall: <https://soundcloud.com/user-429524614/re810225eafc58d18f00ea1baabecaf40d>
- ▶ The scammer’s offer is an attempt to get you to provide your financial information or PII when you provide payment information

Coronavirus Vaccination, Treatment, or Cure Scams

- ▶ **BACKGROUND INFO:** There currently are no vaccines, pills, potions, lotions, lozenges or other prescription or over-the-counter products that prevent, treat or cure the coronavirus.
- ▶ If anyone attempts to sell you a vaccination or other preventative, treatment, or cure by any means, it is a scam
- ▶ Scammers are using their solicitations to steal your financial information or PII

Coronavirus Vaccination, Treatment, or Cure Scams Example

The screenshot shows the 'INFOARS STORE' website. The navigation bar includes links for 'Points', 'Account', 'Wishlist', and 'Cart'. Below the navigation bar, there are categories: 'INFOARS LIFE', 'HEALTH & WELLNESS', 'PREPAREDNESS', 'MEDIA', 'SPECIALS', 'GEAR', and 'SUPPORT US'. The breadcrumb trail reads: 'Home > Health & Wellness > Immune Defense > SuperSilver Whitening Toothpaste'. The product page features a tube of 'SUPER SILVER Whitening Toothpaste' on the left. The main text reads: 'SUPERSILVER WHITENING TOOTHPASTE', 'Introducing the SuperSilver Whitening Toothpaste!', 'Get the perfect combo to start your morning and save on Superblue Bubblegum Toothpaste with the Fluoride-Free Toothpaste Combo!', and 'This product is only intended for use in cleaning or whitening the appearance of teeth. The products on this site are not intended for use in the cure, treatment, prevention or mitigation of any disease, including the novel coronavirus. Any suggestion to the contrary is false and is expressly disavowed.' The price is listed as 'Retail: \$19.95' and 'Now: \$9.95' with a 'Savings: \$10.00 (50%)'. There is a 'Delivery Options' section with 'One Time Delivery - \$9.95' and 'Auto-Ship - \$8.95 With 10% Subscription Discount'. A 'Official website' badge is visible in the bottom right corner.

“The patented nanosilver we have, the Pentagon has come out and documented and Homeland Security has said this stuff kills the whole SARS-corona family at point-blank range. Well, of course it does, it kills every virus.”

[Source: Brighteon.com, Alex Jones Show, March 10, 2020](https://www.brighteon.com/alex-jones-show/march-10-2020)

Coronavirus Vaccination, Treatment, or Cure Scams Example

The screenshot shows a video player interface for 'THE JIM BAKKER SHOW'. The video content is a promotional advertisement for a 'Silver Solution Starter Kit'. The ad features several blue bottles of the product and a sign that reads 'KILLS 99% WITHIN 12 HOURS'. Below the bottles, there is a price tag for '\$125' and contact information: 'PO Box 7330 Brenton, MO 65815'. The video player has a progress bar at the bottom showing 46:37.

THE JIM BAKKER SHOW

Watch Store News About Morningside USA PTL TV Network [Subscribe NOW](#)

KILLS 99% WITHIN 12 HOURS

\$125 Silver Solution Starter Kit (10 1/2 oz. bottles - 20 1/2 oz. tubes - bonus items)
PO Box 7330 Brenton, MO 65815

46:37

A Close Look At What's Not Being Said About The Coronavirus (Day 1)

Pastor Jim and the panel discuss the shocking news about the coronavirus.

Guests: Doctor Sherrill Sellman, Zach Drew, Derek Gilbert, Sharon Gilbert

Coronavirus Vaccination, Treatment, or Cure Scams Example

EXHIBIT A



Due to the recent outbreak for the Coronavirus (COVID-19) the World Health Organization is giving away vaccine kits. Just pay \$4.95 for shipping.

ORDER NOW



JUST PAY \$4.95 FOR SHIPPING

- ▶ “Due to the recent outbreak for the Coronavirus (COVID-19) the World Health Organization is giving away vaccine kits. Just pay \$4.95 for shipping. You just need to add water, and the drugs and vaccines are ready to be administered. There are two parts to the kit: one holds pellets containing the chemical machinery that synthesizes (sic) the end product, and the other holds pellets containing instructions that tell the drug which compound to create. Mix two parts together in a chosen combination, add water, and the treatment is ready.”

Coronavirus Vaccination, Treatment, or Cure Scams Example

Verizon LTE 6:30 PM
Messages Spammer

Paul, scientists just confirmed positive results on testing this Coronavirus protection!
j4est.info/pQHZxxxxxx
Claim a free sample for your family

LTE 6:31 PM
Messages Spammer

Coronavirus alert: This face mask provides an extra layer of safety.
xxxthmsk.com

LTE 6:32 PM
Messages Spammer

Hi Kimberly, no one will be safe from the Coronavirus anymore. This is the only survival guide you require to overcome this crisis
zrt9k.rest/xxxxxx

LTE 6:38 PM
Messages Spammer

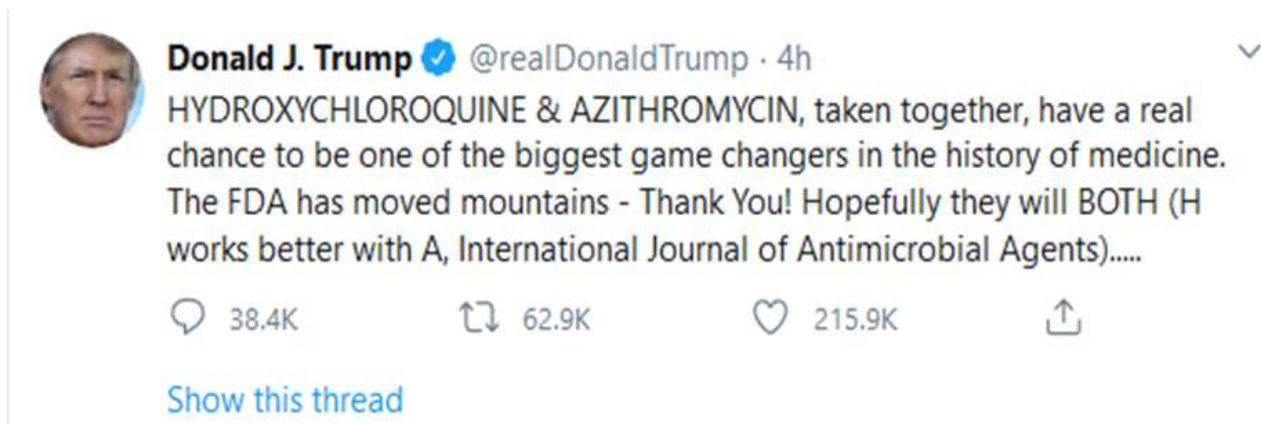
Louise are you and your family prepared for the Corona Virus?
34exxxx.site/bni7niyxxxx
this mask can be ur life line

Coronavirus Vaccination and other Preventatives, Treatment, or Cure Scams Example

- ▶ **BACKGROUND INFO:** There likely is about to be a wave of scams that will purport to sell two drugs, Hydroxychloroquine (and a related drug, Chloroquine) and Azithromycin, as either a preventative measure or “cure” for Covid-19. Both drugs are available in the United States, but they cannot legally be sold online or otherwise without a prescription from a health care professional. While according to Dr. Anthony Fauci, there are no reliable medical studies that demonstrate that these drugs, either alone or in combination, effectively prevent or treat Covid-19, there is limited anecdotal information suggesting they may. On March 30, the FDA granted emergency approval for the use of hydroxychloroquine and chloroquine to treat (but not to prevent) Covid-19, with the caveat that patients to whom they are prescribed should be closely monitored by health professionals because of known serious side-effects from the use of these drugs, including heart arrhythmia.
- ▶ What, therefore, is the basis for predicting this wave of scams?

Coronavirus Vaccination, Treatment or Cure Scams

- ▶ A single tweet, on March 21, which undoubtedly will be cited by many scammers, perhaps as “the one Covid-19 cure endorsed by the President -- now approved by the FDA”:



Coronavirus Vaccination, Treatment or Cure Scams



Coronavirus Charitable Relief Scams

- ▶ **BACKGROUND INFO:** Scams urging people to support disaster victims sadly are both common and pervasive. These scams can be particularly effective because they appeal to and exploit our desire to help others. We know that many people are experiencing significant financial and economic hardships because of the coronavirus pandemic.
- ▶ Charitable relief scams relating to the pandemic are increasing as the pandemic and economic hardships spread
- ▶ Scammers use names that are intentionally and confusingly similar to actual charitable organizations
- ▶ The rise in legitimate crowdfunding makes it more difficult to distinguish what is a legitimate solicitation

Coronavirus Charitable Relief Scams

- ▶ Some general guidelines on charitable giving:
 - ▶ Do not give in to solicitations that demand you make an instant commitment.
 - ▶ Do your research before giving. Check to see if the charity is registered with the Maryland Secretary of State.
 - ▶ Check the charity's rating from the Better Business Bureau at www.give.org.
 - ▶ Call the charity directly to make sure it has authorized the solicitor to collect donations on its behalf.
- ▶ If you decide to donate, make our donation using a credit card (not your debit card) because your liability for fraud on credit cards is limited to \$500. Be aware that if the charity is a scam and your credit card information is stolen you still may suffer numerous inconveniences.

Scams Related to Products in Short Supply

- ▶ Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell supplies currently in high demand, such as surgical masks, nitrile gloves, hand sanitizers, and maybe even toilet paper
- ▶ These scammers may:
 - ▶ At best, take your money and provide you with nothing in return
 - ▶ Use the payment information to access to your credit card or bank accounts
 - ▶ Place malware on your computer
- ▶ The best way to avoid possible scams is to buy local or through a legitimate online retailer
- ▶ If you make a purchase, use a credit card instead of your debit card

Scams Directed at Those More Vulnerable to Coronavirus

- ▶ Generally similar to the short supply scams
- ▶ Scammers may offer to go grocery shopping, run to pharmacy, etc.
- ▶ Some scammers wearing lab coats or scrubs may come to a person's door, identify themselves as being from the local health department or the CDC, and state that the person must be tested for coronavirus because they are in a high-risk category. The scammer's may even attempt to swab the person's nose to take a sample.
- ▶ Scammers will demand immediate payment for the test and sometimes claim they also need PII for their records

Scams Related to Government Stimulus Checks

- ▶ **BACKGROUND INFO:** The federal government will be providing stimulus checks to qualified US citizens. There also will be a special SBA loan program for small businesses.
- ▶ These stimulus programs may generate the following scams:
 - ▶ Emails or robocalls stating that you are eligible for the program and offering to get you your money now, in return for a payment of a fee, rather than waiting for the government to send the check. One scam uses the email address: “uscovid19treasure@gmail.com,” with subject line “COVID-19 PANDEMIC STIMULUS PACKAGE”
 - ▶ An offer to expedite the payment by arranging that consumer receives a direct deposit rather than a check if you provide PII or a checking account number.
 - ▶ Offering to determine your eligibility for a stimulus check or SBA loan in return for payment of a fee.

Scams Playing Off Fear of the Corona Virus

- ▶ Scams may involve coronavirus-related investment opportunities or products not directly related to coronavirus
- ▶ Examples:
 - ▶ Invest in silver because it's an anti-viral
 - ▶ Invest in an alleged pharmaceutical company that makes anti-malarial drugs
 - ▶ Invest in a company that makes or sells quinine (tonic) water
 - ▶ Unrelated products:

Text Message
Today 1:17 PM

Because of the COVID-19 outbreak we are giving out free iPhone 11 smartphones to help you spend time at home: Katie, go to appie10.info/DI7uxPFI0t

Anti-Scam Actions by the Federal Government

- ▶ The Federal Trade Commission and Food and Drug Administration jointly sent warning letters to seven companies allegedly selling unapproved products that may violate federal law by making deceptive or scientifically unsupported claims about their ability to treat coronavirus: (1) Vital Silver; (2) Quinessence Aromatherapy Ltd.; (3) N-ergetics; (4) GuruNanda, LLC; (5) Vivify Holistic Clinic; (6) Herbal Amy LLC; and (7) The Jim Bakker Show.
- ▶ The United States Department of Justice (DOJ) obtained an injunction taking down a website, coronavirusmedicalkit.com, that purported to offer free World Health Organization “vaccine kits” in return for a \$4.95 shipping fee. In its complaint, the DOJ alleged that the scammers were actually using the website “to obtain credit card and other personal information from victims for purposes of engaging in fraudulent purchases and identity theft.”
- ▶ The FBI arrested for file fraud a California scammer who, through an online video, sought investors for his company that he claimed: created a “patent pending cure” for Covid-19; was about to go into mass production; and featured Magic Johnson was a member of the company’s board. He promised a minimum return of \$200-\$300 million on a \$1 million investment. The video was viewed over 633,000 times.

Reporting Scams

- ▶ For all types of fraudulent solicitations from any source:
 - ▶ Federal Trade Commission: www.ftc.gov (click on “File a Consumer Complaint” on upper right-hand side of home page)
 - ▶ Maryland Attorney General’s Consumer Protection Division: http://www.marylandattorneygeneral.gov/Pages/CPD/immFraud/immFraud_complaint.aspx
 - ▶ National Center for Disaster Fraud hotline: 866-720-5721
- ▶ For fraud directed at the elderly:
 - ▶ Elder Fraud Hotline, 833-FRAUD-11 (833-372-8311)
- ▶ For internet-based fraudulent solicitations:
 - ▶ Federal Bureau of Investigation Internet Crime Complaint Center: www.ic3.gov

Final Comments

- ▶ Scammers will exploit any situation they think will create an environment for a successful scam. The coronavirus provides scammers with a platform that preys on people's fears and could make them more likely to be victimized.
- ▶ Be aware that scammers are attempting to use malicious emails, texts, websites, apps, robocalls, and even door-to-door visits to steal financial information and PII from consumers. Scammers are likely to come up with new methods that attempt to exploit the worldwide fear of coronavirus.
- ▶ You can avoid falling prey to this type of scams by remembering these three tips:
 - ▶ Avoid opening attachments and clicking on links within emails or texts from senders that you don't recognize.
 - ▶ Refuse to supply financial information or PII to anyone that you don't know.
 - ▶ Hang up on robocallers without saying anything or touching any buttons.